

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2703

(01/2009)

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS
AND NEXT-GENERATION NETWORKS

Next Generation Networks – Security

The application of AAA service in NGN

Recommendation ITU-T Y.2703

ITU-T Y-SERIES RECOMMENDATIONS

**GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-
GENERATION NETWORKS**

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2703

The application of AAA service in NGN

Summary

Recommendation ITU-T Y.2703 provides an application of authentication, authorization and accounting (AAA) for NGN release 1.

Source

Recommendation ITU-T Y.2703 was approved on 23 January 2009 by ITU-T Study Group 13 (2009-2012) under the WTSA Resolution 1 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2009

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	General concepts for the AAA service	2
6.1	Overview	2
6.2	The AAA process	2
6.3	AAA procedure	3
7	Application model for authentication and authorization in NGN	3
8	AAA architecture in NGN	5
8.1	User to network access	6
8.2	User to network service attachment	7
8.3	Authentication and authorization of user for access to 3rd party service.....	7
9	Enrolment	8
10	Authentication	8
10.1	Authentication entities.....	8
10.2	Procedure for authentication.....	8
11	Authorization	10
11.1	Authorization aspects for NGN	10
11.2	Authorization entities	10
11.3	Procedure for authorization	10
12	Accounting.....	11
12.1	Security accounting	11
12.2	Functions for security accounting	11
Appendix I – Authentication protocol for AAA in NGN		13
I.1	EAP protocol for AAA service in NGN.....	13
I.2	AAA protocols.....	14
Appendix II – X.509 digital certificates as credentials.....		15
Appendix III – Authentication and authorization use-case.....		16
III.1	Authentication and authorization of user for network access	16
III.2	NGN service provider authentication and authorization of user for access to service/application.....	18
III.3	User authentication and authorization of NGN providers	20

	Page
III.4 NGN provider authentication and authorization of 3rd party service/application provider	21
III.5 Use of 3rd party authentication and authorization service	22
Bibliography.....	24

Recommendation ITU-T Y.2703

The application of AAA service in NGN

1 Scope

This Recommendation describes an application for authentication, authorization and accounting (AAA) for next generation networks (NGNs) based on [b-ITU-T Y.2201]: NGN release 1 requirements, [b-ITU-T Y.2012]: Functional requirements and architecture of the NGN release 1 (FRA), [b-ITU-T Y.2701]: Security requirements for NGN release 1, and [b-ITU-T Y.2702]: NGN authentication. This Recommendation applies to the authentication, authorization and accounting process in accessing an NGN using the AAA client and AAA server. In particular, this Recommendation addresses the accounting function only from the standpoint of its contribution to security accounting.

The scope of this Recommendation is:

- 1) The enrolment process.
- 2) Authentication functions and procedures.
- 3) Authorization functions and procedures.
- 4) Security-accounting functions and procedures.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation makes use of the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.811]: The provision of assurance of the claimed identity of an entity.

3.1.2 authentication certificate [b-ITU-T X.811]: A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.

3.1.3 authentication information [b-ITU-T X.811]: Information used for authentication purposes.

3.1.4 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.5 claimant [b-ITU-T X.811]: An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

3.1.6 security audit trail [b-ITU-T X.800]: Data collected and potentially used to facilitate a security audit.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 security accounting: The role that tracks security-related actions or events that can be included as resources in the security audit function.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

AAA	Authentication, Authorization and Accounting
AM-FE	Access Management Functional Entity
ANI	Application-to-Network Interface
EAP	Extensible Authentication Protocol
ID	Identity – as defined by the network, service, or entity being accessed
NAS	Network Access Server
NGN	Next Generation Network
NNI	Network-to-Network Interface
NP	Network Provider
OAMP	Operations, Administration, Maintenance, and Provision
RACF	Resource Access Control Function
SCTP	Stream Control Transport Protocol
SR	Service Resource
TAA-FE	Transport Authentication and Authorization Functional Entity
TE	Terminal Equipment
TUP-FE	Transport User Profile Functional Entity
UNI	User-to-Network Interface

5 Conventions

None.

6 General concepts for the AAA service

This clause deals with the basic concepts of AAA.

6.1 Overview

The authentication, authorization and accounting service provides the functions by which a user's identity is verified (authentication), is given access to the services (authorization) and a means by which consumption of resources is measured (accounting).

6.2 The AAA process

The individual processes within the AAA framework are as follows:

Authentication validates the end user's identity prior to permitting network access. The end user presents a set of credentials such as a username/password combination, a security key, a certificate or biometric data (for example, fingerprints). These credentials are normally agreed during the enrolment process. Verification of the credentials leads to the authorization process.

Authorization defines the privileges and services the end user is allowed once network access is granted. This might include providing an IP address or invoking a filter to determine which applications or protocols are supported. Authentication and authorization are performed together in an AAA-managed environment.

Accounting provides the methodology for collecting information about the end user's resource consumption which can then be processed for billing, auditing, and capacity-planning purposes. Certain accounting data is relevant to the development of a security audit trail.

These three processes are centralized into a set of functions which together provide access control.

6.3 AAA procedure

The AAA service system is composed of an AAA server and an AAA client.

The AAA server has access to a database of user profiles and configuration data. It communicates with AAA clients residing on network components such as NAS (network access server) and routers, to provide distributed AAA services.

The AAA service scenarios are summarized in the following steps:

- The end user connects to the point-of entry device and requests access to the network.
- The AAA client forwards the end user's identity/authentication credentials to the AAA server.
- The AAA server authenticates the user based on the credentials. If authentication is successful, the server then determines which service(s) are authorized and returns an accept or reject response and other relevant data to the AAA client.
- The AAA client notifies the end user that access to specified resources has been granted or denied.

The AAA client sends an accounting message to the AAA server during connection set-up and termination for record collection and storage.

7 Application model for authentication and authorization in NGN

This Recommendation is based on security requirements for NGN in [b-ITU-T Y.2701] and the NGN authentication reference model in [b-ITU-T Y.2702]. The NGN authentication reference model (Figure 7-1) depicts eight authentication reference points; three of which are considered/taken into account by this Recommendation:

They are:

- (1) access of user to network;
- (2) access of user to network provided service;
- (4) access of service provider to receiving user.

Reference points (1) and (4) refer to transport of user traffic and may be viewed as depending on "horizontal" access control at the transport control level, whereas reference points (2) and (8) may be viewed as depending on control data between the transport and service control layers and therefore as being "vertical." This relationship is displayed in Figure 7-2.

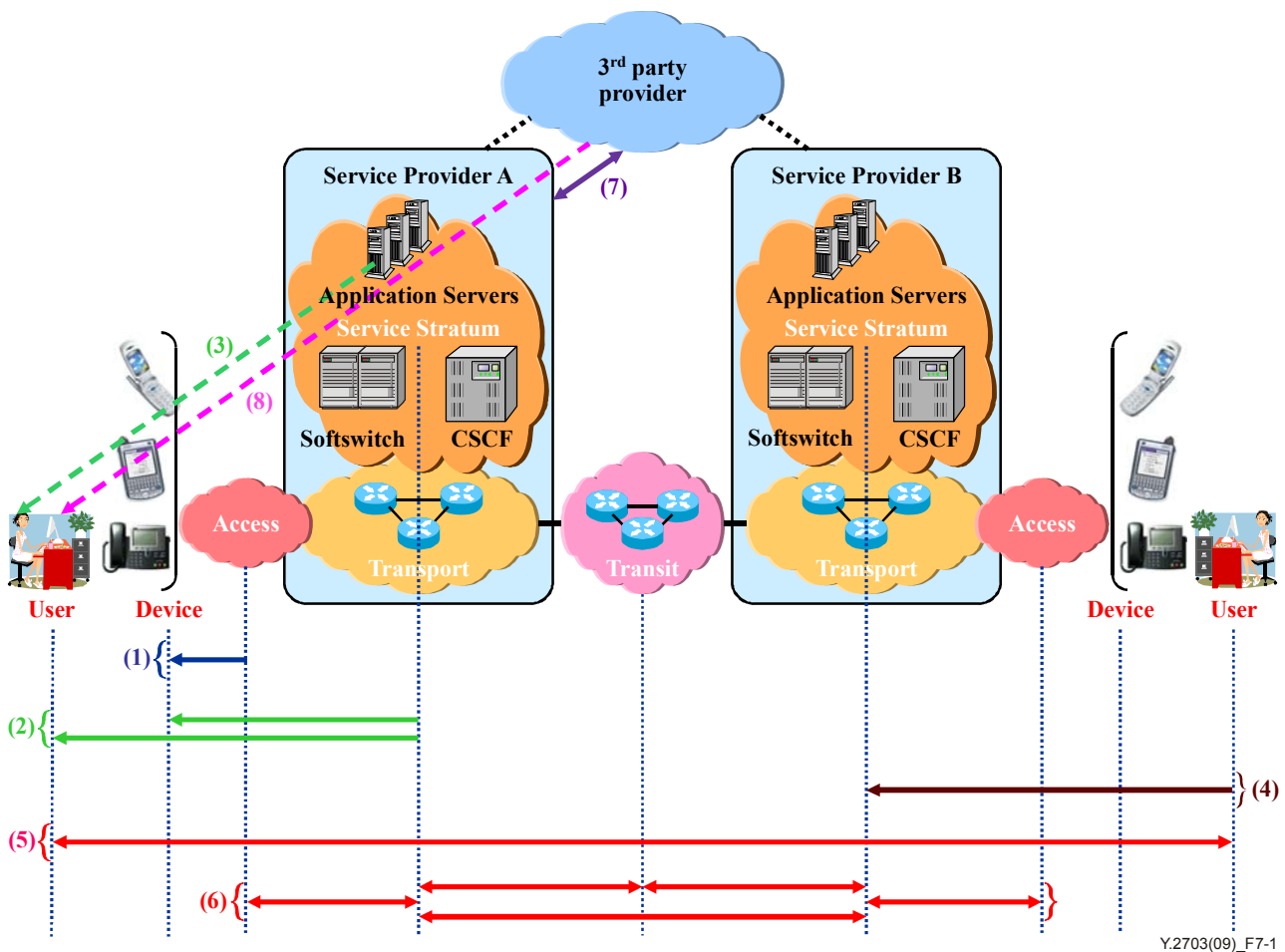


Figure 7-1 – End-to-end reference architectural model (Y.2702 NGN authentication)